TESTIMONY OF
THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

JUNE 9, 2006

Good afternoon, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Energy. I am pleased to be here today to share with the Committee a summary of the actions the Department of Energy is taking to strengthen its cyber security posture.

The Department of Energy takes cyber security very seriously. Our senior management team is working together to ensure that we are taking all appropriate actions to protect our information systems and the information processed on these systems. We are taking a risk-based approach, managing the overall risk and the risk that still remains after all appropriate managerial and technical controls have been applied, often called residual risk.

The Department's cyber security program is guided by the Federal Information Security Management Act (FISMA), including its emphasis on certifying and accrediting every information system before it is placed into operation, by the Committee on National Security Systems (CNSS ), and by the National Industrial Security Program Operating Manual established by Executive Order 12820 for national security systems. Based on a

risk assessment and a system security plan, each system has controls applied to ensure availability, confidentiality, and integrity of each system and the information on that system. These controls are tested to ensure they are working properly. After the controls are applied, a statement of the residual risk is presented to an accrediting official. This official makes the determination for the system to become operational based on this residual risk evaluation and the role of the system in supporting the Agency's mission.

I would like to point out to the Committee that there is no such thing as "no risk" and no such thing as perfect cyber security. Well-informed judgments have to be made as to the nature and amount of protection that is to be applied to each system and network, and that is the nature of the certification and accreditation process. We are also guided in managing cyber security by Office of Management and Budget (OMB) policy and by guidance issued by the National Institute of Standards and Technology (NIST).

Our cyber security program responds to risk assessments conducted within the bounds of our assessment of the current threat to our systems. The threat to our systems from outside our perimeter and from insiders is continually increasing. The hackers and others intent on harming our systems or obtaining information from our systems are becoming smarter in their attacks. The threat is especially challenging given the vulnerabilities in off-the-shelf operating system and applications software that we must use to support our mission.

This software is very complex, and vulnerabilities are continually identified over the lifetime of that software. Although software vendors prepare and distribute software patches after vulnerabilities are identified, there is always a delay in preparing and distributing these software patches, creating a "window" for attacks despite best efforts to maintain secure system configurations and despite best efforts to apply the new software patches in a timely way. I should also point out that software patches need to be tested first before being applied to our systems to ensure that they do not interfere with the systems' ability to meet mission requirements.

Our cyber security posture is bolstered by the testing we do during the certification and accreditation process, and by systematic, continuous vulnerability testing. We also benefit from the testing that the Department's Office of Inspector General conducts as part of its financial and FISMA reviews, and we are also fortunate to have within the Department the Office of Security and Safety Performance Assurance, which conducts Red Team attacks and penetration testing on our systems and networks to identify vulnerabilities, and performs cyber security assessments and evaluations.

The Department of Energy has extensive expertise in the area of cyber security, and we are devoting substantial resources to this important area. The challenge in managing cyber security is for us to prioritize our efforts using a risk-based approach as we implement all the key parts of a balanced cyber security program. We need to be smart about how we apply our cyber security resources, both in what we do and in the relative priority we give to the various parts of this effort.

When I came on board at Energy, at the end of November 2005, the Department had recognized the cyber security challenge it faced, and I have given cyber security the highest priority in the management of the Department's information technology. We had a recently prepared Cyber Security Project Team report in hand at the time that summarized the kinds of actions needed to be taken to improve our cyber security posture.

At the direction of the Secretary and the Deputy Secretary, I led the development of a Department of Energy Cyber Security Revitalization Plan, which now provides the basis for the Department's cyber security program. This plan was developed under the oversight of an Executive Steering Committee, which I chair, and which has as members our Under Secretaries, the Administrator of NNSA and the Under Secretary for Energy Science, and Environment, as well as the Director of the Office of Science, the Director of the Office of Security and Safety Performance Assurance, the Administrator of the Energy Information Administration, and a representative for the Department's Power Marketing Administrations. We have a Cyber Security Working Group that reports to the Steering Committee that has coordinated the development of the Revitalization Plan and is actively involved now in coordinating implementation of the Plan.

In developing this Revitalization Plan, we went "back to basics," guided by FISMA, OMB policy, and NIST guidance. We considered the Department's mission and the way the Department is structured, and we considered the cyber security risks currently faced

by the Department. We factored into the Plan the recommendations from the Cyber Security Project Team report.

Under the Revitalization Plan, the Office of the Chief Information Officer (OCIO) develops top-level cyber security policy, to be issued by the Deputy Secretary. OCIO issues guidance on implementing cyber security management, Department-wide, working with the Cyber Security Working Group in doing so. Our office also leads the charge for awareness by everyone in the Department of the importance of each person's role in cyber security, and provides oversight of the entire Department-wide cyber security program. We also regularly advise senior Department management of evolving threats and the best protection strategies to employ in implementing cyber security protections.

Each of the Under Secretaries establishes policies and implementation plans for their part of the Department, consistent with the overall Departmental policy and guidance. They each tailor their implementation to meet the needs of their respective programs. OCIO works with the entire Department in preparing reports of cyber security status, as required under FISMA, and OCIO also conducts compliance reviews relative to policy and guidance to ensure that adequate protection of our information and information systems is in place. The Office of the Inspector General and the Office of Security and Safety Performance Assurance each conduct appropriate oversight reviews and testing that help ensure that the cyber security program is working as intended. The results of these reviews are expected to continue to be very important inputs to the Department as we continue to improve our cyber security program.

The Revitalization Plan identifies five high priority activities: certification and accreditation; use of an enterprise defense-in-depth strategy, providing layered protection from the perimeter of our networks to our users; asset management, to ensure that all information technology assets are identified and managed well with secure configuration controls and timely software updates; network interconnection and segmentation; and education and awareness. The major components of the revitalization process are identified as: planning, based on a common understanding of risk and threat, to ensure that cyber security is integrated through business practices and Under Secretarial missions; cyber security policy and guidance; architecture and technology that supports Department-wide implementation; common services that support the entire Department, including incident management, education and awareness training, and asset management tools and support; and performance measurement, providing a clear and consistent means to measure the cyber security status of the Department.

The Plan is intended to provide a basis for a long-term, strengthened cyber security program, with a significant beginning to be accomplished in the first twelve months, by February 2007. The highest priority activities, based on risk, are receiving attention and resources first, even as detailed planning and implementation continues throughout the Department. We have already issued revised certification and accreditation guidance, and we have initiated a corporate asset management process. Network segmentation plans have been developed and implementation has begun. We have organized a Department-wide cyber forensics team that is responding daily to cyber attacks, with

excellent results. Cyber security awareness for all employees has been jump started with special bulletins containing detailed guidance, focusing on social engineering attacks, against which everyone's participation is essential.

The Secretary has said that "revitalizing our cyber security program is the best way to ensure that we continue to protect our Department's assets and the nation," and he has charged the Department's leadership to commit ourselves to this task. We are all working together to move as quickly as we can to improve the Department of Energy cyber security posture, and I believe our progress is now being felt through an improved ability to thwart attacks and to bring all the necessary resources to bear quickly and effectively as needed. We understand that cyber security is a never-ending process, and we are committed to maintaining a high level of vigilance to ensure that the Department is able to carry out its mission without disruption caused by cyber threats. I would be pleased to respond to any questions you may have.